

# Likewise<sup>®</sup> Case Study

**Solving Mixed Network Drudgery; How Switching to Centrally Managed User Names and Passwords Saved Valuable Time and Improved Security For a Large Provider of Natural Gas**

Manny Vellon, CTO



**26 words, 144 characters**



- Longest book title: (1,433 characters; 290 words)
- Longest song title: (305 characters; 52 words)
- Longest movie title: (208 characters; 41 words)
  - **Night of the Day of the Dawn of the Son of the Bride of the Return of the Revenge of the Terror of the Attack of the Evil, Mutant, Alien, Flesh Eating, Hellbound, Zombified Living Dead Part 2: In Shocking 2-D**

- Challenges of running heterogeneous systems
- Case study particulars
- How Likewise solved the problem
- Outcomes

- Microsoft Windows
  - End user (desktops, notebooks)
  - Back office (Exchange, AD, Sharepoint)
  - .NET Intranet apps
- “UNIX”
  - Web-facing applications (Apache, etc.)
  - Production databases
  - Line-of-business applications (SAP, MRP, etc.)

Windows™

# UNIX

- Windows

- + Easy to use
- + Applications availability
- + Standard
- Vulnerable
- Monopoly
- I hate Vista

- UNIX

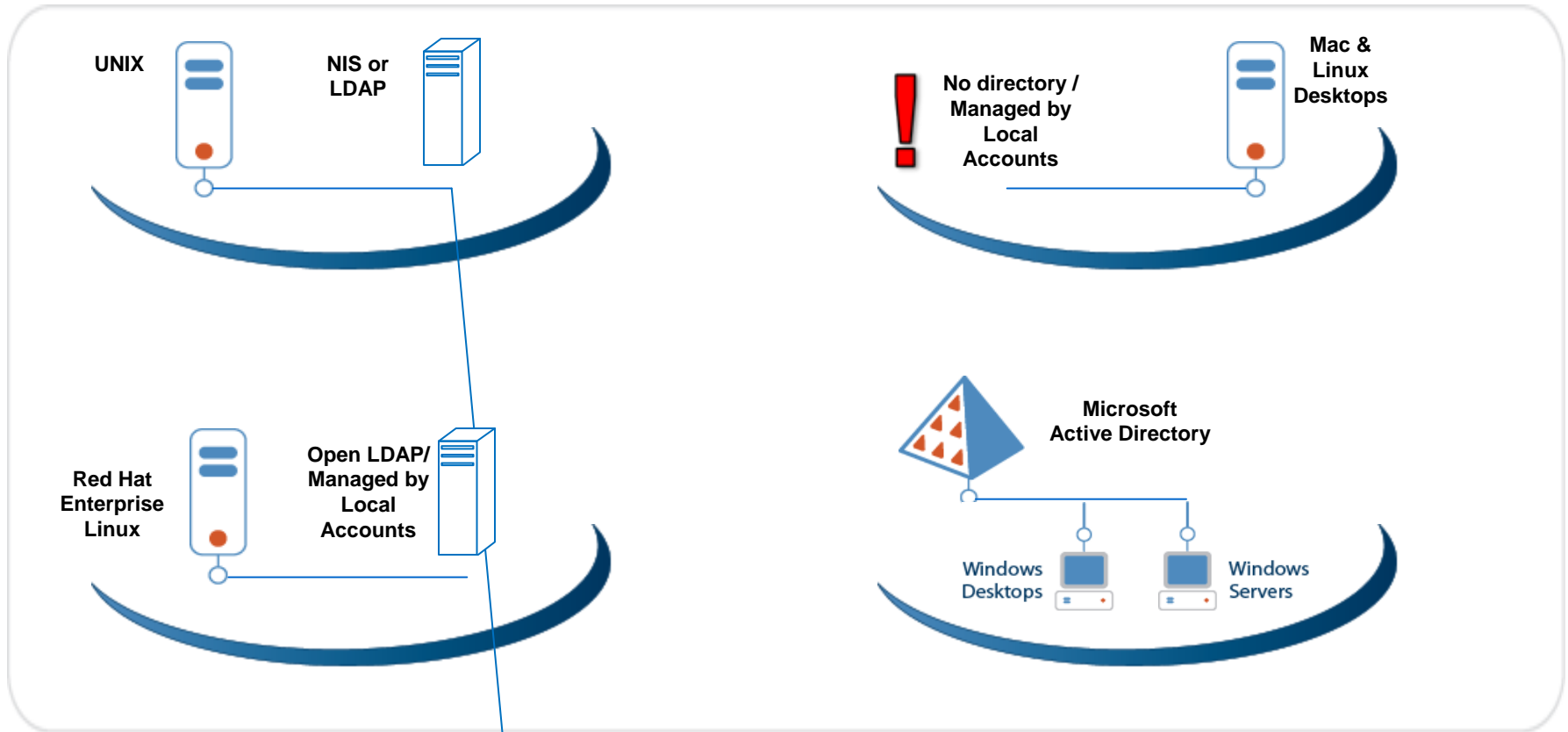
- + More secure
- + Multi-vendor
- + A “real” OS
- Difficult to use
- Not standard
- Costly to administer

Although UNIX is used in applications requiring strong security...

...companies frequently employ poor security practices when managing these systems.

# The Sorry State of Authentication Infrastructure

At Best:



# The Sorry State of Authentication Infrastructure

Most often:

UNIX



No Directory /  
Managed by  
Local  
Accounts



No Directory /  
Managed by  
Local  
Accounts



Mac &  
Linux  
Desktops

Red Hat  
Enterprise  
Linux



No Directory /  
Managed by  
Local  
Accounts



Microsoft  
Active Directory

Windows  
Desktops



Windows  
Servers



- No dominant player; only NIS has any market share
- NIS and NIS+ no longer supported. NIS not secure. Many companies discontinuing use
- Installing and maintaining a directory can be expensive and complicated
- Commercial solutions may lack key features: global deployment, high-availability, laptop support, etc.

95% of F1000 already *have* a central directory handling the bulk of their authentication needs: Active Directory.

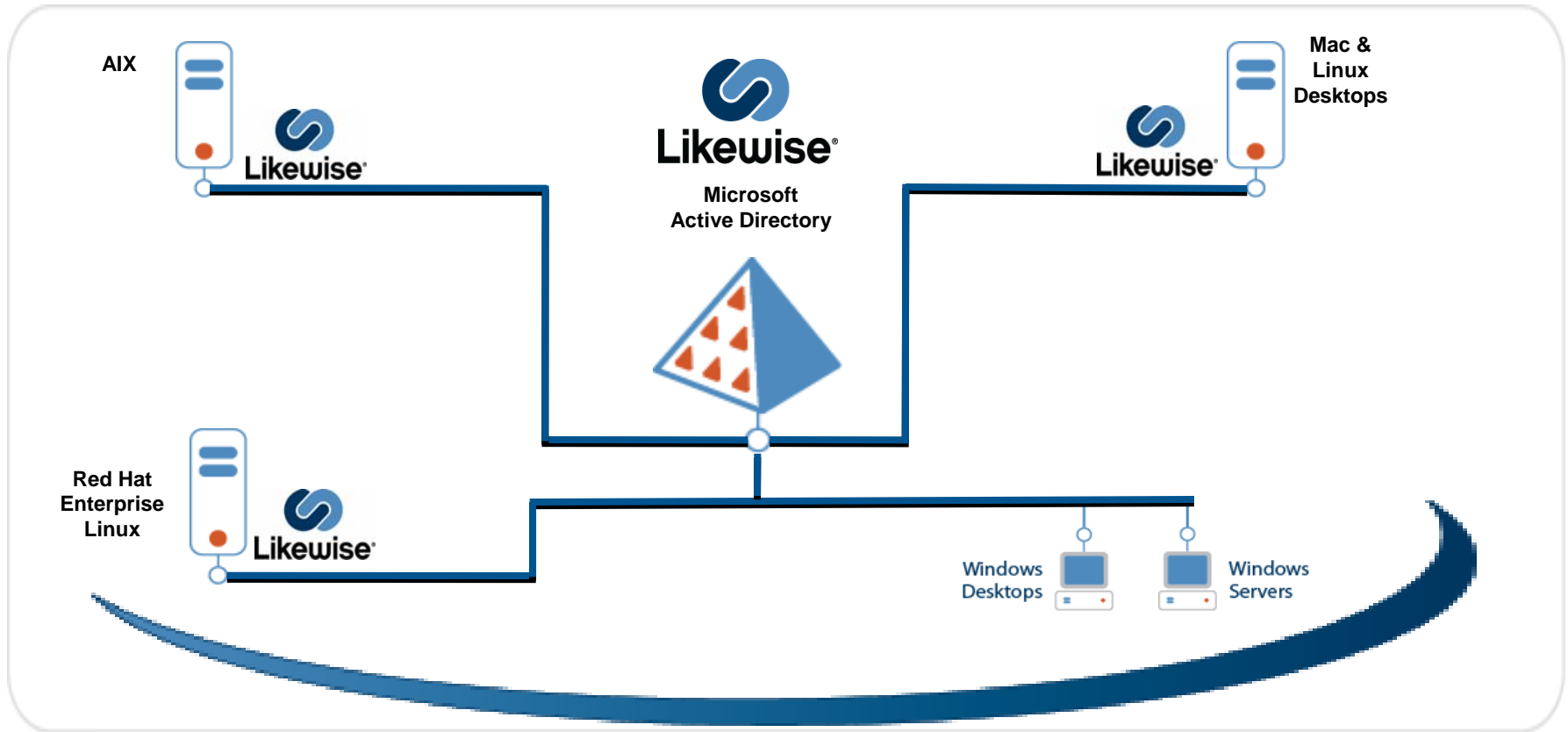
# Case Study: Pikachu\* Energy Corporation

- One of the largest producers of natural gas in the U.S.
- >4,000 employees
- ~100 Linux computers (Red Hat 3, 4, 5)
- Dozens of additional IBM AIX computers
- All user authentication through local /etc/passwd files

\*Not the *actual* name of the company

- User adds, deletes and password changes required operations on multiple systems; time-consuming and error-prone processes
- Failures to remove defunct employee accounts led to security vulnerabilities
- Excessive burden of account management led to frequent use of shared utility accounts (frequently, *root*)
- OS limitations precluded company-wide username and password standards

## Enterprise-wide Authentication, Group Policy, and Reporting



- Likewise is an open source, identity management company that integrates Linux, Unix, and Mac systems into Windows environments
- Areas of benefit:
  - Operational efficiency
  - Audit compliance
  - Security



## Likewise® Open

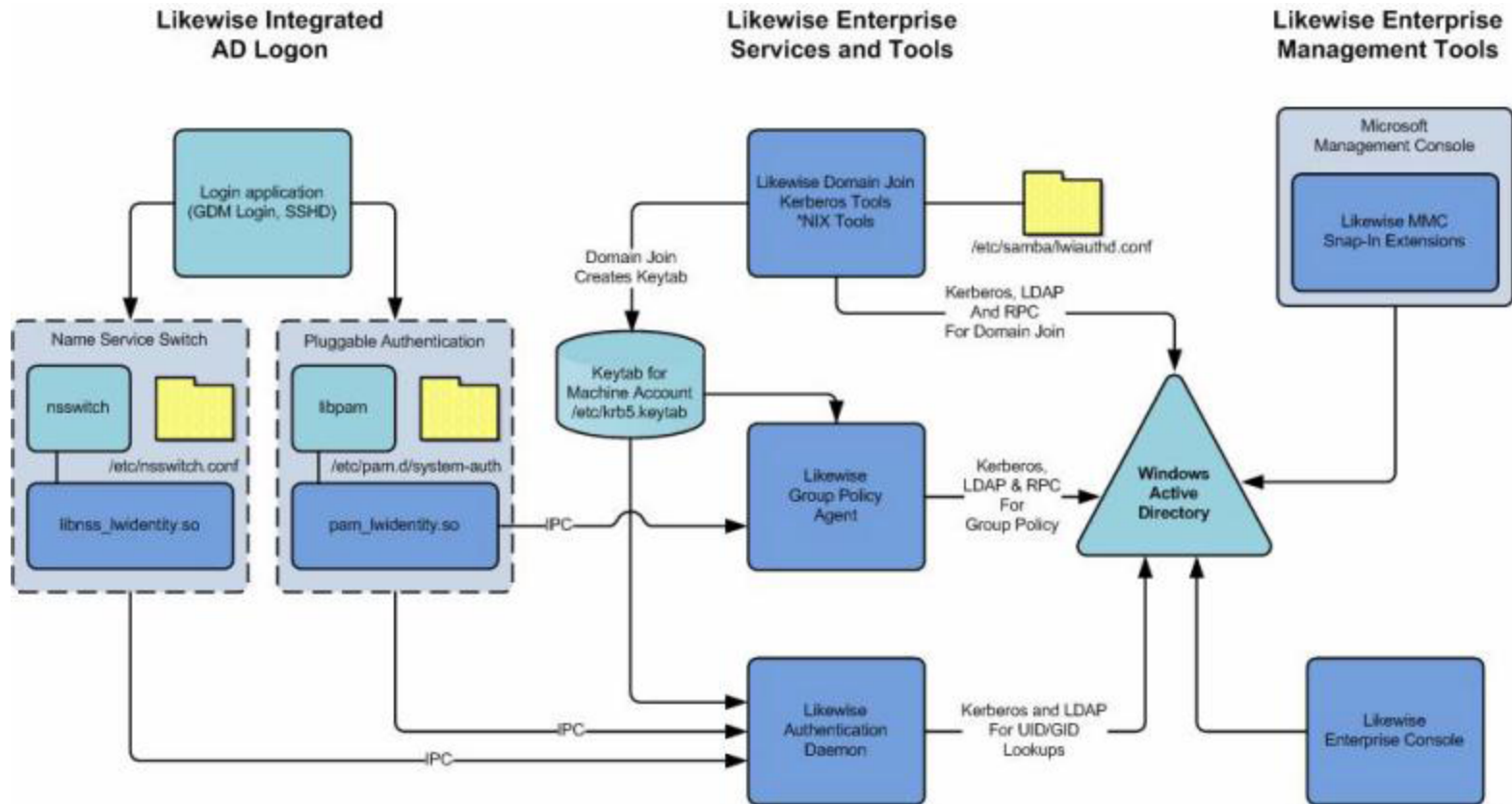
- AD Authentication
- Single User Name & Password
- Kerberos-based SSO
- Enforce User Account and Password Policy

## Likewise® Enterprise

Likewise Open features plus:

- Group Policy support
- Reporting and audit tools
- Centralized user account support
- Account Migration tools
- Windows diagnostics tools

- Integrate all Linux and UNIX authentication with Microsoft AD
- Use Likewise “cell” technology to facilitate administration
- Use Likewise Group Policy for role-based access control and user messaging

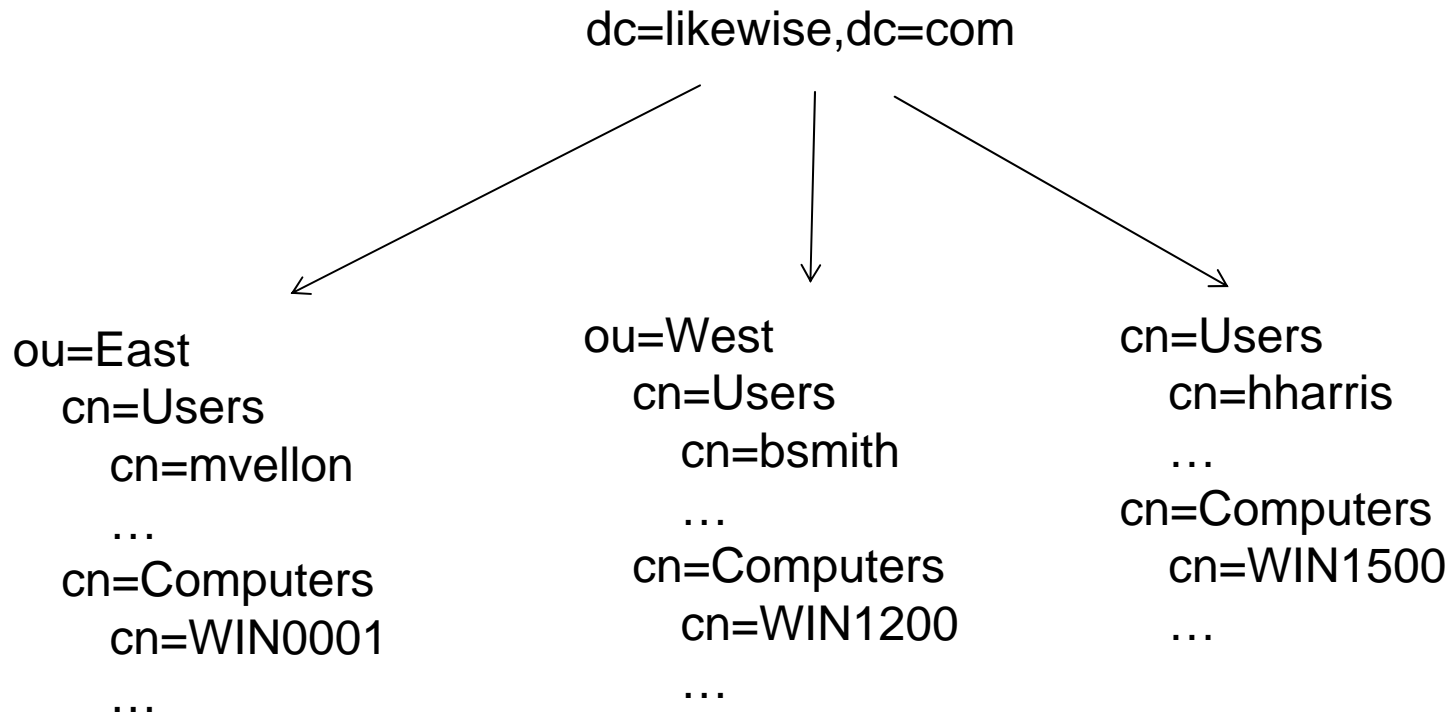


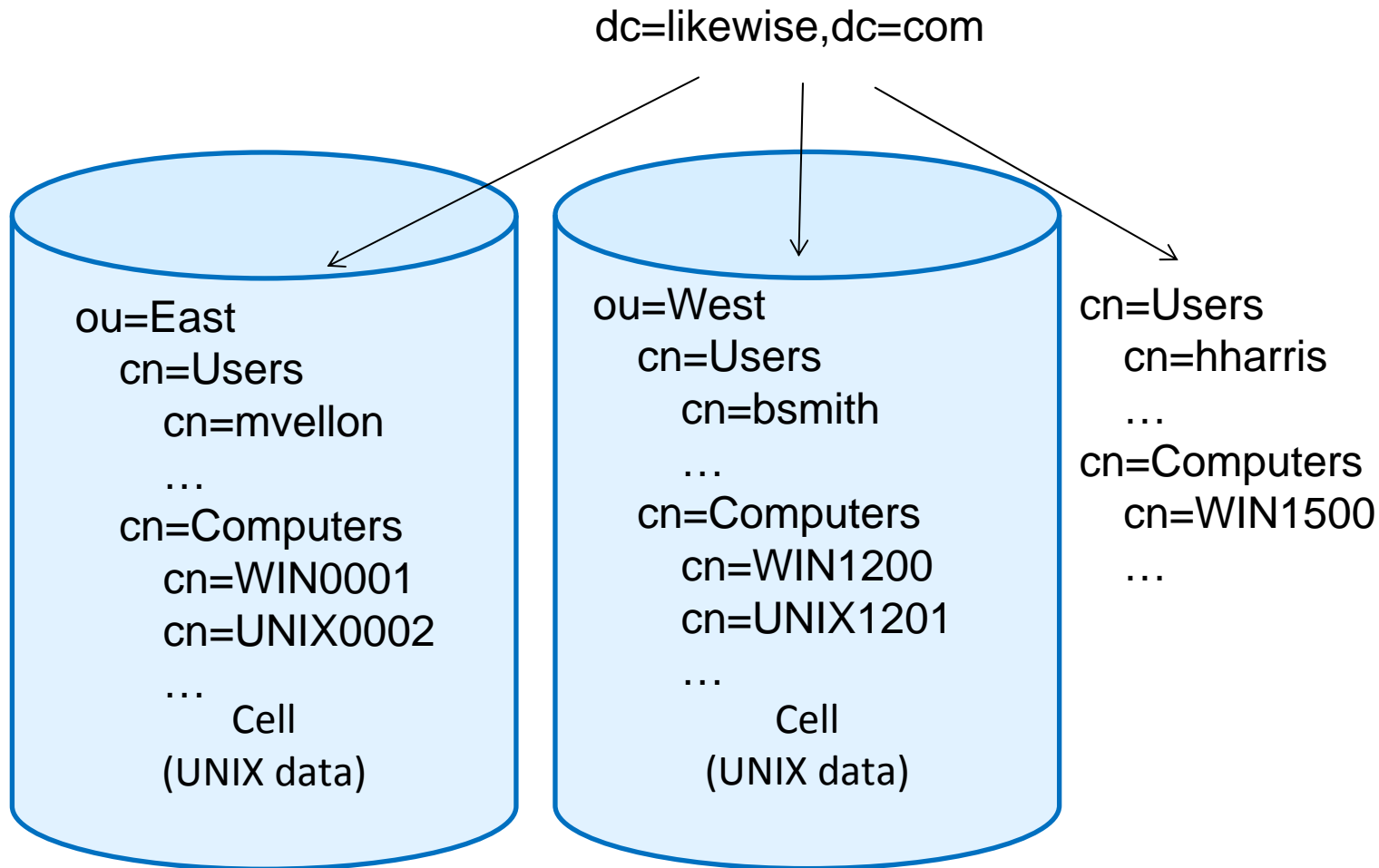
- Likewise is *not* a password synchronization solution
- Likewise adds components to the UNIX authentication pipeline in order to *directly* authenticate users against AD using Kerberos and LDAP protocols
- Likewise adds components to the UNIX name service in order to support name-to-ID mapping (and vice-versa) based on data stored in AD
- Likewise adds components to implement Group Policy on UNIX

# Case Study: Benefits of Integration With AD



- Simplified account management
- Simplified password resets
- Consistent usernames and passwords across company
- Strong passwords across the company
- Consistent security policy across the company
- Better reporting and auditing of user accounts
- No need for synchronization with other account repositories





- Cells facilitate:
  - NIS migration (allow users to have different UNIX attributes when logging into different computers)
  - Access control (a user must be *enabled* in a cell in order to access computers that are “in” the cell)
  - Delegation of duties (can delegate administration of UNIX information without providing full Domain Admin rights)

# Case Study: Benefit of Using Cells

- New OUs added to better manage sites and applications
- Clear delineation of administrative duties of different sites
- Better access control

- Complete analog of Microsoft Windows implementation
- Allows efficient management of thousands of computers by specifying configuration information in a central location (AD)
- Likewise provides an extensible framework for UNIX-specific GP completely integrated with Microsoft tools (GPMC, GPEdit) allowing settings to be easily set, copied, backed-up and restored
- Likewise provides numerous UNIX GP settings: local security policy; *sudo*; *cron*; *syslog*; *motd*; automounts, file/directory download and many more

- Setting “Logon rights (require\_membership\_of)” policy allows user-level or group-level restrictions on what users can access which computers
- Setting “*sudo*” policy facilitates RBAC:
  - Likewise GP framework distributes *sudo* configuration files to relevant computers
  - *sudo* configuration file refers to AD group membership; user access to privileged commands controlled by making them members of specific groups
- Setting *motd* policy and password expiration notification policy lowered calls to help desk

- With *sudo*:
  - Everyone doesn't have to have the *root* password
  - Non-root users can run root-only commands (if they have the appropriate rights configured)
  - Access to root-only commands are logged to *syslog* providing an audit trail
  - Rights can be configured by user name or group membership
  - Name and group membership tests are Likewise-aware
  - Using AD group membership greatly simplifies RBAC

- Greatly simplified account administration
- Consistent usernames and passwords
- Improved delineation of administrative duties
- Improved access control
- Implementation of RBAC through *sudo*
- Fewer calls to helpdesk